SMĚRNICE O NAKLÁDÁNÍ S OSOBNÍMI ÚDAJI

OBECNÍ ÚŘAD ZLATÁ KORUNA

Obsah:

Článek 1
Úvodní ustanovení

Tato Směrnice o nakládání s osobními údaji (dále jen „tato směrnice“ nebo „směrnice“) se vydává na základě Nařízení EU 679/2016 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), někdy také General Data Protection Regulation (dále jen „Nařízení GDPR“).

Článek 2
Předmět, účel a působnost

1. Směrnice stanovuje taková opatření a pravidla, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů spravovaných a zpracovávaných organizací. Ochranou osobních údajů je míněno zajištění důvěrnosti spravovaných a zpracovávaných osobních údajů, jejich integrity, dostupnosti a dalších bezpečnostních aspektů všech osobních údajů v míře potřebné pro činnost organizace a to v souladu s platnou legislativou.
2. Tato směrnice se zabývá ochranou všech osobních údajů ve vlastnictví nebo ve správě organizace, bez ohledu na jejich podobu (tištěnou, psanou, uloženou elektronicky, odesílanou poštou, předávanou elektronicky, ústním podáním, telefonem, faxem apod.).
3. Tato směrnice definuje tzv. systém řízení ochrany osobních údajů, fungující v souladu s dalšími dokumenty:
    - Organizační řád
    - Pracovní řád
    - Spisový řád a skartační plán
4. Tato směrnice je závazná pro všechny osoby organizačně zařazené do struktury organizace a osoby, které osobní údaje zpracovávají na základě smlouvy uzavřené s organizací jakožto správcem osobních údajů (toto ustanovení musí být součástí obsahu uzavřené smlouvy).

Článek 3
Základní pojmy

1. „**osobní údaje**“ - veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“). Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (například jméno, adresa, datum narození, atd.).
2. „**zvláštní kategorie osobních údajů**“ - osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.
3. „**biometrické údaje**“ - osobní údaje týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, například zobrazení obličeje.

4. „**zpracování**“ - jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, které jsou prováděny pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, zpřístupnění, šíření, atd.
5. „**pseudonymizace**“ - zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací.
6. „**anonymizace**“ - zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů.
7. „**správce**“ - organizace jako orgán veřejné moci, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů.
8. „**zpracovatel**“ - fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.
9. „**příjemce**“ - fyzická nebo právnická osoba, orgán veřejné moci, nebo jiný subjekt, kterým jsou osobní údaje poskytnuty.
10. „**souhlas subjektu údajů**“ - jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů;
11. „**záznamy o činnostech zpracování**“ - záznamy vedené organizací o zpracování osobních údajů. Záznamy obsahují účely zpracování, rozsah zpracovávaných osobních údajů, informace o příjemcích daných osobních údajů, lhůtách pro výmaz a popis přijatých technických a organizačních opatření k zajištění bezpečnosti údajů.
12. „**dozorový úřad**“ - Úřad pro ochranu osobních údajů.
13. „**Pověřenec**“ – Pověřenec pro ochranu osobních údajů. Je jmenován starostou obce.

Článek 4
Role, rozsah působnosti

1. Odpovědnost za zajištění ochrany osobních údajů v souladu s Nařízením GDPR nese ředitel organizace.
2. Vedení organizace (ředitel, vedoucí oddělení) odpovídá za to, že pravidla ochrany osobních údajů budou dodržovat zaměstnanci, kteří s osobními údaji jakkoliv nakládají.
3. Pravidla ochrany osobních údajů se vztahují rovněž na všechny další subjekty, které pracují s osobními údaji organizace. Tyto subjekty musí být k dodržování zásad ochrany osobních údajů smluvně zavázány.

Článek 5
Přístup k osobním údajům

K osobním údajům mají přístup pouze takové osoby, které jsou k přístupu oprávněni na základě pracovní smlouvy, pracovní náplně či obdobného dokumentu.

Článek 6
Zásady zpracování osobních údajů

1. Osobní údaje musí být:

a. ve vztahu k subjektu údajů zpracovávány zákonným a transparentním způsobem,
b. shromažďovány pro určité legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný,
c. přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány,
d. přesné a v případě potřeby aktualizované - musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny,
e. uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány,
f. zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným zpracováním a před ztrátou, zničením nebo poškozením.

2. Jsou zpracovávány pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné.
3. Písemnosti obsahující osobní údaje podléhají procesu skartace v souladu se Spisovým řádem a skartačním plánem.

Článek 7
Zákonnost zpracování osobních údajů

1. Organizace jako správce osobních údajů zpracovává pouze takové osobní údaje, jejichž zpracování je zákonné. Zpracování osobních údajů je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:

   a. subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů,
   b. zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů,
   c. zpracování je nezbytné pro splnění právní povinnosti organizace,
   d. zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby,
   e. zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci,
   f. zpracování je nezbytné pro účely oprávněných zájmů organizace.

2. Účel zpracování osobních údajů musí vycházet z výše uvedených právních základů. Osobní údaje nesmějí být použity k jinému účelu, než ke kterému byly získány.
3. Pokud je zpracování založeno na souhlasu subjektu údajů, musí být organizace schopna doložit existenci tohoto souhlasu.

Článek 8
Opatření pro ochranu osobních údajů

1. Zaměstnanec je povinen dodržovat pravidlo čistého stolu (neponechávat volně položené písemnosti obsahující osobní údaje bez dozoru na svém pracovním stole, po ukončení pracovního dne je každý zaměstnanec povinen takové listinné písemnosti uložit do úložných prostor a zajistit tak, aby k nim neměly přístup osoby bez oprávnění).

2. Zaměstnanec je povinen v případě odchodu z kanceláře, kde se již nenachází žádný další zaměstnanec tuto místnost zamknout.
3. Zaměstnanec je povinen v případě přítomnosti cizí osoby v kanceláři a nutnosti odchodu zaměstnance z kanceláře, kde se již nenachází žádný další zaměstnanec, vyprovodit cizí osobu na chodbu, kancelář zamknout a opětovný vstup cizí osoby do kanceláře umožnit až při vlastním návratu do kanceláře (neponechávat cizí osoby bez dozoru v kanceláři).
4. Zaměstnanec je povinen využívat pro elektronické zpracování osobních údajů k tomu určené informační systémy organizace.
5. Zaměstnanec je povinen udržovat písemnosti v elektronické formě obsahující osobní údaje uložené na pevných discích a ve své e-mailové schránce v souladu s lhůtami stanovenými pro zpracování dle Spisového řádu a skartačního plánu a v minimálním rozsahu umožňujícím dosažení účelu zpracování.
6. Zaměstnanec je oprávněn ukládat písemnosti v elektronické formě obsahující osobní údaje pouze na určená datová úložiště.
7. Zaměstnanec je povinen udržovat v tajnosti svá přístupová oprávnění (přihlašovací jméno a heslo) k informačním systémům, tato přístupová oprávnění si nezapisovat (na papír, do souboru, apod.) ani je neprozrazovat žádné další osobě.
8. Zaměstnanec není oprávněn přeposílat písemnosti obsahující osobní údaje na své nebo cizí soukromé emailové schránky.
9. Zaměstnanec není oprávněn zasílat datové soubory obsahující osobní údaje emailem bez jejich dodatečného zabezpečení za pomoci šifrování, přičemž heslo k souboru musí být předáno jiným kanálem (SMS nebo telefonicky).
10. Zaměstnanec je povinen pro předání osobních údajů primárně použít Informační systém datových schránek.
11. Zaměstnanec není oprávněn ukládat na veřejná datová úložiště na Internetu jakékoli datové soubory obsahující osobní údaje.
12. Zaměstnanec není oprávněn provádět na svěřených prostředcích jakékoliv hardwarové zásahy (např. měnit komponenty počítače, připojovat vlastní externí zařízení apod.) a spouštět či instalovat jakýkoliv nepovolený software.
13. Zaměstnanci není dovoleno využívat k přístupu k informačním systémům organizace soukromá mobilní zařízení.
14. Zaměstnanec není oprávněn jakkoliv měnit nastavení, případně vypínat ochranu proti škodlivému kódu (antivirový program apod.) na svěřených prostředcích.
15. Zaměstnanec je povinen využívat pro ukládání listinné dokumentace obsahující osobní údaje (včetně fyzických nosičů elektronické dokumentace) k tomu určené úložné prostory a tyto úložné prostory při opuštění kanceláře uzamknout (pokud lze). Uživatel osobních údajů je povinen písemnostem obsahujícím osobní údaje přiřazovat skartační znaky dle platného Spisového řádu a skartačního plánu.
16. Klíče od určených kanceláří jsou zaměstnancům vydávány prokazatelným způsobem a je vedena evidence vydaných klíčů. Je zajištěno ukládání a zabezpečení náhradních klíčů od kanceláří a úložných prostor.
17. Zaměstnanci nejsou oprávněni hovořit (osobně i telefonicky) o osobních údajích v přítomnosti třetích osob, které nemají právo danou informaci vědět.

Článek 9

Předávání osobních údajů

Osobní údaje mohou být předávány pouze na zákonném základě (viz. článek 7). Předávání se uskutečňuje pouze v legislativně či smluvně stanoveném rozsahu a formátu.

Článek 10
Zveřejňování osobních údajů

Osobní údaje mohou být zveřejňovány pouze na zákonném základě (viz. článek 7). Před zveřejněním jsou osobní údaje anonymizovány v rozsahu zajišťujícím minimalizaci rozsahu zveřejňovaných osobních údajů při dosažení účelu zveřejnění uloženého legislativou (dokumentaci anonymizovat vždy, pokud zákon neukládá jinak). Výjimkou jsou osobní údaje, u kterých je udělen Souhlas subjektu údajů s takovýmto postupem.

Fotografie zaměstnanců organizace se mohou zveřejňovat na webových stránkách organizace apod., pouze po výslovném souhlasu zaměstnance s tímto zveřejněním

Článek 11
Informační povinnost

Naplnění informační povinnosti podle článků 13 a 14 Nařízení GDPR musí být zajištěno zveřejněním náležitých informací na webových stránkách organizace.

Článek 12
Práva subjektu údajů

1. Subjekt údajů může uplatnit tato práva:

    a. přístup k osobním údajům
    b. opravu a výmaz osobních údajů
    c. omezení zpracování osobních údajů
    d. přenositelnost osobních údajů
    e. vznesení námitky
2. Naplnění práv subjektů údajů zajišťuje příslušný zaměstnanec organizace. Ten je oprávněn požádat o součinnost každého dalšího zaměstnance organizace či zpracovatele.
3. Způsob podání žádosti o naplnění práv subjektů údajů je zveřejněn na webových stránkách, případně dalšími vhodnými způsoby.
4. Informace jsou subjektu údajů poskytovány bez zbytečného odkladu a v každém případě ve lhůtě do jednoho kalendářního měsíce od obdržení žádosti. Tuto lhůtu je možné v případě potřeby a s ohledem na složitost a počet žádostí prodloužit o další maximálně dva kalendářní měsíce, kdy subjekt údajů musí být o takovém odůvodněném prodloužení lhůty k poskytnutí údajů informován nejpozději ve lhůtě do jednoho kalendářního měsíce od obdržení žádosti.
5. Informace jsou subjektu údajů poskytovány výhradně na základě prokazatelného jednoznačného ověření totožnosti subjektu údajů (občanský průkaz, datová schránka).

Článek 13
Postup při porušení zabezpečení osobních údajů

1. Zjištění případu porušení zabezpečení osobních údajů ohlásí zaměstnanec neprodleně svému nadřízenému a Pověřenci.

2. Pověřenec ve spolupráci s vedením organizace rozhodne o dalším postupu.
3. Pověřenec následně předloží vedení organizace ke schválení návrh nápravných opatření pro zamezení opakování obdobného porušení zabezpečení osobních údajů. Za realizaci nápravných opatření odpovídá ředitel organizace.

Článek 14
Ohlašování bezpečnostních incidentů

1. Pokud dojde k porušení zabezpečení osobních údajů, musí organizace toto porušení bez zbytného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásit dozorovému úřadu, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Oznamují se jen rizikové incidenty pro práva a svobody fyzických osob, nikoli bagatelní záležitosti, které jsou nerizikové.
2. V oznámení správce subjektu údajů musí popsat povahu porušení zabezpečení, přijatá opatření, pravděpodobné důsledky a též musí sdělit kontaktní údaje na pověřence pro ochranu osobních údajů

Článek 15
Oznamování případů porušení zabezpečení osobních údajů subjektu údajů

Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí organizace toto porušení bez zbytečného odkladu subjektu údajů.

Článek 16
Použití zpracovatele

Zpracování zpracovatelem se řídí smlouvou. Organizace je povinna zajistit, aby s každým zpracovatel byla před zahájením zpracování uzavřena Smlouva o zpracování osobních údajů.

Zpracovatel není oprávněn zapojit do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení organizace.

Článek 17
Závěrečná ustanovení

Tato směrnice nabývá účinnosti dne 25.5.2018.